Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of	
A Samsung Galaxy S20+ 5G cellular phone, model # SM-G986U, Serial # R5CN30CQQMP, IMEI 3555 2511 0884 134, currently located at the FBI Flagstaff Resident Agency in Arizona	Case No. 22-4318MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona (identify the person or describe the property to be searched and give its location):

As further described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

As set forth in Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before September 8, 2022 .
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.
☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge.

Any U.S. Magistrate Judge on duty in AZ .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*) ☐ for days (*not to exceed 30*)
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Camille D. Bibles
Digitally signed by Camille D. Bibles
Date: 2022.08.25 18:14:20 -07'00'
Judge's signature

City and State: Flagstaff, AZ

Honorable Camille D. Bibles, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

RETURN

Case No.: 22-04318MB	Date and Time Warrant Executed:	Copy of warrant and inventory left with:

Inventory Made in the Presence of:

Inventory of the property taken and name of any person(s) seized:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is a cellular phone, specifically a Samsung Galaxy S20+ 5G, model # SM-G986U, Serial # R5CN30CQQMP, IMEI 3555 2511 0884 134. The phone is currently located at the FBI Flagstaff Resident Agency, 5900 S. Pulliam Drive, Flagstaff, AZ 86001.

ATTACHMENT B

Particular Things to be Seized

The following items of evidence, contraband, fruits, and instrumentalities used in and relating to violations of 18 U.S.C. §§ 1153, 1111 (First Degree Murder), and 249 (Hate Crime):

1. Any material or information that describes the planning and preparation of a crime;
2. Any material, information, photographs or diagrams concerning a conspiracy to commit a crime;
3. Any material or information pertaining to a motive to engage in a crime, which includes homophobic and transphobic content;
4. Any information recording BEGAY's schedule, travel, or physical location on June 10 through July 1, 2021;
5. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
6. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

7. Any and all security devices, to include physical keys, encryption devices, "dongles" and similar physical items needed to gain access to computer hardware;
8. Any material associated with or involved in the process of "spoofing" numbers on phone lines;
9. Evidence of the attachment of other devices;
10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
11. Evidence of the times the device was used;
12. Passwords, encryption keys, and other access devices that may be necessary to access the device;
13. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
14. Records of or information about Internet Protocol addresses used by the device;
15. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
16. Records evidencing the use of the Internet; and

17. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

18. As used herein, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

19. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. In addition, peripherals, equipment that send data to, or receive data from, computer hardware, but do not normally store user data, such as keyboards, mice, printers, scanners, plotters, video display monitors, modems, cables, and certain types of facsimile machines; Any and all computer software and storage media to include any material capable of storing

information in a manner that can be used by computer hardware to save and/or retrieve information, such as diskettes, CD-ROM's, CD-R's, CD-Ws, DVD's, DVD-Rs, DVD-RWs, magnetic tapes, ZIP disks, JAZ disks, Peerless disks, SparQ disks, ORB disks, optical disks, smart-cards, EPROMS, and digital memory media such as CompactFlash, SmartMedia, Sony Memory Sticks, USB "thumb" or "key" drives, in addition to computer photographs, Graphic Interchange formats and/or photographs, digital cameras, slides, scanners or other visual depictions of such Graphic Interchange format equipment.

In searching this data, the computer-based personnel may examine and copy all of the data contained in the cellular telephone or digital devices to view their precise contents and determine whether the data falls within the items to be seized. In addition, the computer personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:

A Samsung Galaxy S20+ 5G cellular phone, model # SM-G986U, Serial # R5CN30CQQMP, IMEI 3555 2511 0884 134, currently located at the FBI Flagstaff Resident Agency in Arizona	)	Case No. 22-04318MB

ELECTRONIC APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, F.B.I. Special Agent Louis-Philippe Noel, a federal law enforcement officer for the government, request an electronic search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, hereby incorporated by reference.

located in the District of Arizona, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, hereby incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- [X] evidence of a crime;
- [X] contraband, fruits of crime, or other items illegally possessed;
- [X] property designed for use, intended for use, or used in committing a crime;
- [ ] a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1153, 1111, and 249	Murder and Hate Crime

The application is based upon the following facts:

- [X] Continued on the attached sheet (see attached **Affidavit**).
- [ ] Delayed notice _____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Ryan Powell *Ryan Powell*

Pursuant to 28 U.S.C. § 1746(2), I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 8/25/2022

Louis-Philippe Noel
Applicant's Signature

Louis-Philippe Noel, F.B.I. Special Agent
Printed Name and Title

Sworn by Telephone

Date/Time: _____

Date: _____

Camille D. Bibles

Digitally signed by Camille D. Bibles
Date: 2022.08.25 18:14:50 -07'00'

Judge's Signature

City and State: Flagstaff, AZ

Camille D. Bibles,
United States Magistrate Judge
Printed Name and Title

AFFIDAVIT

I, Louis-Philippe Noel (affiant), a Special Agent of the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows.

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the physical examination of a cellular phone currently in law enforcement possession, and the extraction from the phone of electronically stored information described in Attachment B

2. Your affiant, Louis-Philippe Noel, is a Special Agent (SA) of the FBI, and is currently assigned to the Flagstaff, Arizona Resident Agency of the FBI. I have been employed with the FBI since July 2017. I have been assigned to investigate violent crime on the Navajo Nation Indian Reservation in Arizona. I have received training from the FBI regarding the investigation of violent crime and crimes involving the use of electronic communications.

3. The information contained in this affidavit is based upon my personal knowledge, training, and experience; my consultation with other experienced law enforcement officers; and the investigation by other law enforcement officers. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause to support issuance of the requested search warrant.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1153, 1111

(Murder), and 249 (Hate Crime) have been committed by Trevor Begay (BEGAY). There is also probable cause to search the phone described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the District Court of Arizona is a district court of the United States that has jurisdiction over the offense being investigated.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is a cellular phone, specifically a Samsung Galaxy S20+ 5G, model # SM-G986U, Serial # R5CN30CQQMP, IMEI 3555 2511 0884 134. It is currently located at the FBI Flagstaff Resident Agency, 5900 S. Pulliam Drive, Flagstaff, AZ 86001.

7. The applied-for warrant would authorize the forensic examination of the phone for the purpose of identifying electronically stored data particularly described in Attachment B.

DETAILS OF INVESTIGATION

8. On June 11, 2021, at approximately 08:30 A.M., an individual identified as S.W., an enrolled member of Navajo Nation Indian Tribe, was found deceased on the Navajo Nation Indian Reservation, in an open field 4.5 miles west of mile post 480 off

Arizona State Highway 89A, in Cameron, Arizona. S.W. appeared to have suffered head trauma.

9. FBI Agents arrived on scene at approximately 11:40 A.M. (Flagstaff Local Time). When Agents arrived, the deceased had been removed and transported to the Coconino County Office of the Medical Examiner. FBI Agents processed the scene and collected shoe impressions and vehicle tire impressions.

10. On June 11, 2021, an FBI Agent used a mobile biometrics application to positively identify the deceased as S.W.

11. On June 14, 2021, an FBI Agent and Navajo Nation Criminal Investigator (CI) interviewed S.W.'s mother, K.N., who explained that S.W. was born as a male but identified as a female and went by a female name.

12. K.N. provided S.W.'s cell phone number as (808) 217-6414. S.W. had a black iPhone and had her own cellular account and did not share a cellular plan with anyone. S.W. typically communicated with family members by text messages or phone calls. S.W. always had her cell phone and would never leave it behind.

13. S.W. lived in Gap, Arizona, with her mother and sister. On Thursday, June 10, 2021, S.W. left the residence in Gap and told K.N. she was "just going up the road" and would return. At approximately 11:00 P.M., S.W. returned to the residence in Gap to retrieve her bag. K.N. heard what sounded like a loud truck outside. S.W. told K.N. that she was going to Red Lake.

14. K.N.'s granddaughter, K.G., spoke with and provided a ride to S.W. around 2:00 A.M. on Friday, June 11, 2021. S.W. contacted K.G. from her cell phone and said she was "stranded in Red Lake." S.W. used her phone to share her location with K.G. S.W. said she wanted to meet a friend at the store in Red Lake and that her friend was coming from Tuba City to pick her up. K.G. took S.W. to the store and saw a blue GMC pickup truck parked at the store as they arrived. The truck was lifted, had tinted windows, big tires, and an LED light bar mounted on top of the windshield. S.W. got into the pickup truck and the truck drove off.

15. When S.W.'s body was found on June 11, 2021, her phone and bag were not located with her body.

16. On June 14, 2021, an autopsy was performed on S.W. The full report was received on September 9, 2021. The postmortem examination showed S.W. had multiple blunt force head injuries, including multiple (7) scalp lacerations, extensive abrasions and superficial lacerations of the face, a skull fracture, and multiple areas of bruising of the brain (cortical contusions). Additional injuries included multiple sharp force injuries including an incised wound of the neck, a stab wound of the right shoulder, and multiple incised wounds of the hands, and multiple abrasions and contusions on the upper and lower extremities. The death was classified as a homicide and attributed to blunt force craniocerebral injuries.

17. On June 14, 2021, an FBI Agent served a preservation letter to Verizon for cellular number (808) 217-6414 and obtained a search warrant for the phone number.

18. On June 17, 2021, an FBI Agent received the search warrant returns for S.W.'s phone number and reviewed the information. According to the phone records, a phone call was made to S.W.'s phone by (928) 890-4564 on June 11 at approximately 1:09 A.M. The call is the last incoming call to S.W.'s phone.

19. Agents conducted a database search for (928) 890-4564 and discovered that the number was associated with 1625 N. West St. in Flagstaff, Arizona.

20. On June 30, 2021, FBI Agents drove past 1625 N. West St. in Flagstaff, Arizona, and observed a blue GMC Sierra parked in the driveway.

21. FBI Agents searched vehicle records and discovered that a 2010 GMC Sierra with Arizona license plate number CNF5059 and VIN 3GTRKTE32AG267210 is registered to BEGAY at 1625 N. West St. in Flagstaff, Arizona.

22. On June 30, 2021, FBI Agents obtained a search warrant for the truck. While executing the search warrant, FBI Agents interviewed BEGAY. He gave consent for his phone to be searched and provided his passcode.

23. On July 12, 2021, a logical extraction was conducted on BEGAY's phone. A logical extraction is the process of extraction through the Application Programming Interface (API) communicating with the mobile device operating system to request data.

24. On July 15, 2021, FBI Agents interviewed I.S. I.S. admitted to partaking in the assault that resulted in the death of S.W. I.S. said that he had been electronically communicating with S.W. through Instagram using BEGAY's phone. The conversations were sexual in nature. I.S. asked for a photo of S.W.'s genitals, and S.W. responded that

she was transgendered. When BEGAY learned this information, he became furious and said he and I.S. needed to teach S.W. a lesson.

25. According to I.S., BEGAY and I.S. arranged to meet S.W. They picked her up in BEGAY's truck. They stopped at a remote location and BEGAY pulled S.W. out of the truck by her hair. BEGAY hit and kicked S.W. and beat her with the metal handle to a jack. As BEGAY attacked S.W., he was saying homophobic slurs. I.S. also hit and kicked S.W. BEGAY and I.S. transported S.W. to a second location in the desert in the bed of BEGAY's truck. They left S.W. there. They had blood on their clothes. They drove BEGAY's truck to BEGAY's grandparents' house. They were in possession of S.W.'s phone. BEGAY and I.S. changed clothes and then drove to a remote area to burn their clothes as well as S.W.'s phone. I.S. took agents to the location, and the agents observed and collected burned clothes and what appeared to be the burned remains of a phone.

26. On March 24, 2022, FBI Agents interviewed I.S., who stated BEGAY previously deleted everything on his phone, to include e-mails. BEGAY told I.S. the importance of deleting e-mails, because e-mails could contain social media content.

27. The FBI currently has BEGAY's phone in its possession. BEGAY previously gave his consent for the FBI to search his phone, and the FBI performed a preliminary logical extraction of BEGAY's phone. The FBI now wishes to perform a more thorough search of BEGAY's phone, namely a physical extraction. Because BEGAY's consent to search his phone was provided more than a year ago, I seek this additional

warrant out of an abundance of caution to be certain that an examination of the phone will comply with the Fourth Amendment and other applicable laws.

28. In my training and experience, I know that the phone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the phone first came into the possession of the FBI.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer/Laptop: A computer consists of the hardware or physical components of the equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Computer hardware includes but is not limited to any data processing units, memory typewriters, and self-contained "laptop" or "notebook" computers; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, flash or "thumb" drives, and other memory storage devices; peripheral input/output devices such as keyboards, printers, scanners, plotters, video display monitors, and optical readers, and related communication devices such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplets, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices; as

well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as physical keys and locks.

b. Software. Computer software is digital information that interpreted by a computer and any of its related components to direct the way the components work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating system applications like word processing, graphics, or spreadsheet programs, and utilities, source code, object code, compilers, interpreters, and communications programs.

c. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience, and research, I know that cellular phones such as BEGAY's have capabilities that allow them to serve as a wireless telephone, PDA, portable media player, and internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. When extracting data from a mobile device, there are several levels of extractions that can be performed. A logical extraction is the fastest and most widely supported extraction available using forensic software; however, it is also the most limited. A logical extraction will generally have access to SMS/MMS messages, contacts, calendars, call logs, images, and video/audio files. A logical extraction relies on the mobile device operating system to obtain data. On the other end of the spectrum is a physical extraction. A physical extraction is the most extensive data acquisition but also the least supported by forensic software. A physical extraction makes a copy of the data present on the mobile device and does not rely on the operating system to determine what it can access. In addition to obtaining everything that

is available in a logical extraction, a physical extraction may also obtain files, hidden files, and deleted data.

33. There is probable cause to believe that things that were once stored on BEGAY's phone may still be stored there, for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used

it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. Forensic evidence: As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how BEGAY's phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the phone because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

35. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of BEGAY's phone consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

36. Manner of execution: Because this warrant seeks only permission to examine evidence already in the FBI's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

37. Based upon your affiant's training, experience, and observations, there is probable cause to believe that BEGAY's phone contains information and data constituting evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1153, 1111 (Murder), and 249 (Hate Crime).

38. Based on the forgoing information, I request that the Court issue the proposed search warrant authorizing examination of the device described in Attachment A to seek the information described in Attachment B.

39. **Pursuant to 28 U.S.C. § 1746(2), I declare that the foregoing is true and correct to the best of my knowledge and belief.**

Dated: 8/25/2022

Special Agent Louis-Philippe Noel
Federal Bureau of Investigation

Subscribed and sworn to telephonically this _____ day of August 2022.

Camille D. Bibles

Digitally signed by Camille D. Bibles
Date: 2022.08.25 18:15:25 -07'00'

HONORABLE CAMILLE D. BIBLES
United States Magistrate Judge
District of Arizona

ATTACHMENT A

Property to Be Searched

The property to be searched is a cellular phone, specifically a Samsung Galaxy S20+ 5G, model # SM-G986U, Serial # R5CN30CQQMP, IMEI 3555 2511 0884 134. The phone is currently located at the FBI Flagstaff Resident Agency, 5900 S. Pulliam Drive, Flagstaff, AZ 86001.

ATTACHMENT B

Particular Things to be Seized

The following items of evidence, contraband, fruits, and instrumentalities used in and relating to violations of 18 U.S.C. §§ 1153, 1111 (First Degree Murder), and 249 (Hate Crime):

1. Any material or information that describes the planning and preparation of a crime;
2. Any material, information, photographs or diagrams concerning a conspiracy to commit a crime;
3. Any material or information pertaining to a motive to engage in a crime, which includes homophobic and transphobic content;
4. Any information recording BEGAY's schedule, travel, or physical location on June 10 through July 1, 2021;
5. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
6. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

7. Any and all security devices, to include physical keys, encryption devices, "dongles" and similar physical items needed to gain access to computer hardware;
8. Any material associated with or involved in the process of "spoofing" numbers on phone lines;
9. Evidence of the attachment of other devices;
10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
11. Evidence of the times the device was used;
12. Passwords, encryption keys, and other access devices that may be necessary to access the device;
13. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
14. Records of or information about Internet Protocol addresses used by the device;
15. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
16. Records evidencing the use of the Internet; and

17. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

18. As used herein, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

19. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. In addition, peripherals, equipment that send data to, or receive data from, computer hardware, but do not normally store user data, such as keyboards, mice, printers, scanners, plotters, video display monitors, modems, cables, and certain types of facsimile machines; Any and all computer software and storage media to include any material capable of storing

information in a manner that can be used by computer hardware to save and/or retrieve information, such as diskettes, CD-ROM's, CD-R's, CD-Ws, DVD's, DVD-Rs, DVD-RWs, magnetic tapes, ZIP disks, JAZ disks, Peerless disks, SparQ disks, ORB disks, optical disks, smart-cards, EPROMS, and digital memory media such as CompactFlash, SmartMedia, Sony Memory Sticks, USB "thumb" or "key" drives, in addition to computer photographs, Graphic Interchange formats and/or photographs, digital cameras, slides, scanners or other visual depictions of such Graphic Interchange format equipment.

In searching this data, the computer-based personnel may examine and copy all of the data contained in the cellular telephone or digital devices to view their precise contents and determine whether the data falls within the items to be seized. In addition, the computer personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.